PART 3:
Criteria Group Checklists

The following checklists are designed to help you gather information about the information system(s) in your organization. It is divided into five main criteria groups as follows: *System Documentation, System Security, Audit Trails, Disaster Planning and Recovery* and *Metadata*. These criteria groups are explained in detail in Part 2 of this manual. An introductory section, *Questions to Consider*, and a supplementary section on *Data Warehousing* are also included here.

Complete the criteria from beginning to end for total system evaluation or, depending on your agency's needs, select those criteria groups that require review. How you proceed is entirely up to you. You can use the *Top Level Criteria* below and/or the *Legal Risk Analysis Tool* to help you select the applicable criteria checklists.

Top Level Criteria The following criteria should be used to establish a trustworthy information system. If you are unsure or unable to answer Yes to any of the following questions, go to the Criteria Group listed and complete the detailed analysis.	**In Place? Yes/No**	**Notes**
1. System administrators should maintain complete and current documentation of the entire system. *If unsure, go to **Criteria Group 1** to do an analysis of your documentation procedures.*		
2. System administrators should establish, document, and implement security measures. *If unsure, go to **Criteria Group 2** to do an analysis of your security procedures.*		
3. System administrators should establish audit trails that are maintained separately and independently from the operating system. *If unsure, go to **Criteria Group 3** to do an analysis of your audit procedures.*		
4. System administrators should establish a comprehensive disaster recovery plan. *If unsure, go to **Criteria Group 4** to do an analysis of your disaster recovery procedures.*		
5. Each record should have an associated set of metadata. *If unsure, go to **Criteria Group 5** to do an analysis of your metadata procedures.*		

Questions to Consider	Response
What laws and/or regulations (state and federal) apply to the data within your system?	
What are your industry's standards for system security?	
What are your industry's standards for data security?	
What areas/records might lawyers target?	
What areas/records might auditors target?	
What data is of permanent/historical value to you? To others?	

Criteria Group 1: System Documentation System Documentation Questions	Response
What is the system's unique identifier and/or common name?	
What is the agency and department(s) responsible for the system?	
What is the agency and department(s) responsible for applications?	
What is the name and contact information of the person(s) responsible for system administration?	
What is the name and contact information of the person(s) responsible for system security?	
Has a formal risk assessment of the system been completed? Date? Performed by? Methodology? Findings?	
Were design reviews and system test run prior to placing the system in production? Were the tests documented?	
Is application software properly licensed for the number of copies in use?	
If connected to external systems lacking commensurate security measures, what mitigation procedures are in place?	
What other systems might records be migrated to?	

Criteria Group 1 Checklist (1.A-1.B.)

System Documentation Analysis (e.g., specifications, program manuals, user guides) included in retention schedules, retained for as long as the longest retention time applicable to the records produced in accordance with the documents

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
1.A.1 System Documentation: hardware procurement			
1.A.1 System Documentation: hardware installation			
1.A.1 System Documentation: hardware modifications			
1.A.1 System Documentation: hardware maintenance			
1.A.1 System Documentation: use of only agency-authorized hardware			
1.A.2 System Documentation: software procurement			
1.A.2 System Documentation: software installation			
1.A.2 System Documentation: software modification			
1.A.2 System Documentation: software maintenance			
1.A.2 System Documentation: use of only agency-authorized software			
1.A.3 System Documentation: communication networks procurement			

Criteria Group 1 Checklist (1.A-1.B.)

System Documentation Analysis (e.g., specifications, program manuals, user guides) included in retention schedules, retained for as long as the longest retention time applicable to the records produced in accordance with the documents

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
1.A.3 System Documentation: communication networks installation			
1.A.3 System Documentation: communication networks modifications			
1.A.3 System Documentation: communication networks maintenance			
1.A.4 System Documentation: interconnected systems (including the Internet) — list			
1.A.4 System Documentation: interconnected systems — names and unique identifiers			
1.A.4 System Documentation: interconnected systems — owners			
1.A.4 System Documentation: interconnected systems — names and titles of authorizing personnel			
1.A.4 System Documentation: interconnected systems — dates of authorization			
1.A.4 System Documentation: interconnected systems — types of connections			
1.A.4 System Documentation: interconnected systems — indication of system of record			

Criteria Group 1 Checklist (1.A-1.B.)

System Documentation Analysis (e.g., specifications, program manuals, user guides) included in retention schedules, retained for as long as the longest retention time applicable to the records produced in accordance with the documents

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
1.A.4 System Documentation: interconnected systems — sensitivity levels			
1.A.4 System Documentation: interconnected systems — security mechanisms, security concerns, personnel rules of behavior			
1.B.1 System Documentation: programming conventions and procedures			
1.B.2 System Documentation: development and testing procedures, including tools			
1.B.2 System Documentation: development and testing procedures — periodic functional tests should include anomalous as well as routine conditions and be documented such that they are repeatable			
1.B.3 System Documentation: applications and associated procedures for entering and accessing data			
1.B.3 System Documentation: applications and associated procedures for data modification			
1.B.3 System Documentation: applications and associated procedures for data duplication			
1.B.3 System Documentation: applications and associated procedures for data deletion			

Criteria Group 1 Checklist (1.A-1.B.)

System Documentation Analysis (e.g., specifications, program manuals, user guides) included in retention schedules, retained for as long as the longest retention time applicable to the records produced in accordance with the documents

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
1.B.3 System Documentation: applications and associated procedures for indexing techniques			
1.B.3 System Documentation: applications and associated procedures for outputs			
1.B.4 System Documentation: identification of when records become official			
1.B.5 System Documentation: record formats and codes			
1.B.6 System Documentation: routine performance of system backups — appropriate labels			
1.B.6 System Documentation: routine performance of system backups — secure, off-line, off-site storage			
1.B.6 System Documentation: routine performance of system backups — periodic integrity tests			
1.B.7 System Documentation: routine performance of quality assurance and control checks (incl. audit trails)			
1.B.7 System Documentation: routine performance of quality assurance and control checks — identification devices (e.g., security cards) periodically checked to ensure proper functioning and correctness of identifying information and system privilege levels			

Criteria Group 1 Checklist (1.A-1.B.)

System Documentation Analysis (e.g., specifications, program manuals, user guides) included in retention schedules, retained for as long as the longest retention time applicable to the records produced in accordance with the documents

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
1.B.7 System Documentation: routine performance of quality assurance and control checks — storage mediums undergo regular statistical sampling following established procedures outlining sampling methods, identification of data loss and corresponding causes, and the correction of identified problems			
1.B.8 System Documentation: migration of records to new systems and media as necessary, with all record components managed as a unit throughout transfer			
1.B.9 System Documentation: standard training for all users and personnel with access to equipment			
1.B.9 System Documentation: standard training — users should sign statements agreeing to terms of use			

Criteria Group 2: System Security System Security Questions	Response
Who can invoke change mechanisms for object, process, and user security levels?	
Who (creator, current owner, system administrator, etc.) can grant access permission to an object after the object is created?	
Is there a help desk or group that offers advice and can respond to security incidents in a timely manner?	
Is system performance monitoring used to analyze system performance logs in real-time to look for availability problems, including active attacks and system and network slowdowns and crashes?	
List internal and external user groups and the types of data created and accessed.	
Have all positions been reviewed with respect to appropriate security levels?	
What are the procedures for the destruction of controlled-access hardcopies?	
How is information purged from the system?	
How is reuse of hardware, software, and storage media prevented?	

Criteria Group 2 Checklist (2.A-2.C.)
System Security Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
2.A.1 System Security — User Authorization: user identification and access procedures should be established and documented			
2.A.1 System Security — User Authorization: users should be authenticated prior to being granted access			
2.A.2 System Security — User Authorization: unique identifier and password for each user			
2.A.2 System Security — User Authorization: identifiers and passwords not used more than once within a system			
2.A.2 System Security — User Authorization: use of access scripts with embedded passwords limited and controlled			
2.A.2 System Security — User Authorization: upon successful log-in, users should be notified of date and of last successful log-in, location of last log-in, and each unsuccessful log-in attempt on user identifier since last successful entry			
2.A.2 System Security: where identification codes in human-readable form are too great a security liability, use of other forms such as encoded security cards or biometric-based devices			
2.A.3 System Security — User Authorization: password rules include minimum password length, expiration dates, and limited number of log-on attempts			

Criteria Group 2 Checklist (2.A-2.C.)
System Security Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
2.A.3 System Security — User Authorization: determination of what level and frequency of log-on error constitutes a misuse problem which, in turn, would trigger notification of security personnel			
2.A.4 System Security — User Authorization: users restricted to only level of access necessary to perform their job duties			
2.A.5 System Security — User Authorization: permission to alter disposition/retention codes, and/or to create, modify, and delete records granted only to authorized users with proper clearance			
2.A.5 System Security — User Authorization: modification of record identifiers prohibited			
2.A.6 System Security — User Authorization: Access to private keys for digital signatures limited to authorized personnel			
2.A.7 System Security — User Authorization: maintenance of lists of all current and past authorized users along with their privileges and responsibilities			
2.A.7 System Security — User Authorization: current list of users reviewed on a regular schedule to ensure timely removal of authorizations for former employees, and adjustment of clearances for workers with new job duties			

Criteria Group 2 Checklist (2.A-2.C.)
System Security Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
2.A.8 System Security — User Authorization: personnel duties and access restrictions arranged such that no individual with an interest in record content will be responsible for administering system security, quality controls, audits, or integrity-testing functions.			
2.A.8 System Security — User Authorization: No individual should have the ability to single-handedly compromise the system's security and operations			
2.B.1 Internal System Security: access to system documentation controlled and monitored			
2.B.2 Internal System Security: access to output and storage devices controlled and monitored			
2.B.3 Internal System Security: controls in place to ensure proper security levels of data when archiving, purging, or moving from system to system			
2.B.3 Internal System Security: controls in place for the transportation or mailing of media or printed output			
2.B.4 Internal System Security: procedures for the complete sanitization and secure disposal of hardware when no longer needed.			
2.B.4 Internal System Security: procedures for the complete sanitization and secure disposal of software when no longer needed			

Criteria Group 2 Checklist (2.A-2.C.)
System Security Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
2.B.4 Internal System Security: procedures for the complete sanitization and secure disposal of storage media when no longer needed			
2.B.4 Internal System Security: documentation of sanitization and secure disposal should include date, equipment identifiers, methods, personnel names			
2.B.5 Internal System Security — insecurity-detection mechanisms constantly monitoring the system			
2.B.5 Internal System Security: fail-safes and processes to minimize the failure of primary security measures in place at all times			
2.B.6 Internal System Security: security procedures and rules reviewed on a routine basis to maintain currency			
2.B.7 Internal System Security — Access: measures in place to guard system's physical security			
2.B.7 Internal System Security — Access: measures in place to guard system's physical security — access to rooms with terminals, servers, wiring, backup media			
2.B.7 Internal System Security — Access: measures in place to guard system's physical security — data interception			
2.B.7 Internal System Security — Access: measures in place to guard system's physical security — mobile/portable units such as laptops			

Criteria Group 2 Checklist (2.A-2.C.)
System Security Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
2.B.7 Internal System Security — Access: measures in place to guard system's physical security — structural integrity of building			
2.B.7 Internal System Security — Access: measures in place to guard system's physical security — fire safety			
2.B.7 Internal System Security — Access: measures in place to guard system's physical security — supporting services such as electricity, heat, air conditioning, water, sewage, etc.			
2.B.8 Internal System Security: security administration personnel undergo training to ensure full understanding of the security system's operation			
2.C.1 External System Security: additional security measures employed in cases of remote access, especially through public telephone lines (e.g., input device checks, caller identification checks (phone caller identification), callbacks, security cards)			
2.C.2 External System Security: for records originating outside of the system, the system should be capable of verifying their origin and integrity			
2.C.2 External System Security: non-system records — verification of sender or source			
2.C.2 External System Security: non-system records — verification of the integrity, or detection of errors in the transmission or informational content of record			

Criteria Group 2 Checklist (2.A-2.C.)
System Security Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
2.C.2 External System Security: non-system records — detection of changes in the record since the time of its creation or the application of a digital signature			
2.C.2 External System Security: non-system records — detection of viruses or worms			

Criteria Group 3: Audit Trails Audit Trail Questions	Response
Who can access audit data?	
Who can alter audit data?	
Who can add audit data?	
Who can delete audit data?	
How can the audit logs be read?	
Who can read audit data?	
What tools are available to output audit information? What are the formats?	
Who can output audit information?	
What mechanisms are available to designate and change activities chosen for audit?	
Who is able to designate and change activities chosen for audit?	
How are audit logs protected?	

Criteria Group 3 Checklist (3.A-3.D.)
Audit Trail Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
3.A Audit Trails: if audit trails are encoded to conserve space, the decode mechanism must always accompany the data			
3.A.1 Audit Trails — General Characteristics: audit trail software and mechanisms subject to strict access controls			
3.A.1 Audit Trails — General Characteristics: audit trail software and mechanisms protected from unauthorized modification			
3.A.1 Audit Trails — General Characteristics: audit trails protected from circumvention			
3.A.2 Audit Trails — General Characteristics: audit trails backed up periodically onto removable media to ensure minimal data loss in case of system failure			
3.A.3 Audit Trails — General Characteristics: system automatically notifies system administrators when audit storage media nearing capacity. Response documented			
3.A.3 Audit Trails — General Characteristics: when storage media containing audit trail is physically removed from the system, the media should be physically secured as required by the highest sensitivity level of the data it holds			
3.B Audit Trails — System to track password Usage and Changes			

Criteria Group 3 Checklist (3.A-3.D.)
Audit Trail Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
3.B Audit Trails — Password Usage and Changes: user identifier			
3.B Audit Trails — Password Usage and Changes: successful and unsuccessful log-ins			
3.B Audit Trails — Password Usage and Changes: use of password-changes procedures			
3.B Audit Trails — Password Usage and Changes: user ID lock-out record			
3.B Audit Trails — Password Usage and Changes: date of password use			
3.B Audit Trails — Password Usage and Changes: time of password use			
3.B Audit Trails — Password Usage and Changes: physical location of user			
3.C Audit Trails — Users: system in place to log and track users and their online actions			
3.C Audit Trails — Users: system in place to log and track users and their online actions — details of log-in (date, time, physical location, etc.)			
3.C Audit Trails — Users: system in place to log and track users and their online actions — creation of files/ records			

Criteria Group 3 Checklist (3.A-3.D.)
Audit Trail Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
3.C Audit Trails — Users: system in place to log and track users and their online actions — accessed file/record identifiers and accompanying activity (deletion, modification, change of sensitivity/security level, etc.)			
3.C Audit Trails — Users: system in place to log and track users and their online actions — accessed device identifiers			
3.C Audit Trails — Users: system in place to log and track users and their online actions — software use			
3.C Audit Trails — Users: system in place to log and track users and their online actions — production of printed output			
3.C Audit Trails — Users: system in place to log and track users and their online actions — overriding of human-readable output markings (including overwrite of sensitivity label markings and turning-off of labeling mechanisms) on printed output			
3.C Audit Trails — Users: system in place to log and track users and their online actions — output to storage devices			
3.C Audit Trails — Users: users made aware that their use of computerized resources is traceable			

Criteria Group 3 Checklist (3.A-3.D.)
Audit Trail Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
3.D Audit Trails: Logged for each record by audit trails: user identifier			
3.D Audit Trails: Logged for each record by audit trails: record identifier			
3.D Audit Trails: Logged for each record by audit trails: date			
3.D Audit Trails: Logged for each record by audit trails: time			
3.D Audit Trails: Logged for each record by audit trails: usage (e.g., creation, capture, retrieval, modification, deletion)			

Criteria Group 4: Checklist
Disaster Planning and Recovery

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
4.A Disaster Plan: periodically reviewed for currency and tested for efficiency			

Criteria Group 5: Metadata Metadata Questions	Response
What are the current components of a complete or final record of the transaction?	
What are the minimal components necessary to provide evidence of the transaction? (If you went to court, what would be the minimum information you would need?)	
Are there any laws, regulations, or professional best practices that specify the structure (including medium, format, relationships) of the record of the transaction or any of its components?	
What information is necessary to interpret the contents of the record?	
During which agency business processes might you have to access this record?	
Who are the external secondary users of the record?	
What are the rules, laws, and regulations that restrict or open access to these records to external users?	
How will the record be reproduced to meet the needs of internal and external secondary users? What are the reproduction formats?	
Is there a mechanism in place to indicate sensitivity level on hardcopies? Who can enable/disable this function?	
What are your industry's standards for records retention?	
What is the records disposition plan?	
Who is responsible for authorizing the disposition of records?	
Who is responsible for changes to the records disposition plan?	

Criteria Group 5: Metadata Metadata Questions	Response
How does the system accommodate integration of records from other systems?	
Who can access metadata?	
Who can alter metadata?	
Who can delete metadata?	
Who can add metadata?	
Does system automatically assign unique consecutive numbers and time-date stamps to the individual units of storage media as they are written to for the first time to prevent the addition of false units or the removal of legitimate ones from the storage series?	
Does the system automatically assign new identifiers to modified records?	
If the records are not individually authenticated, does the record series metadata include the name or title of the individual responsible for validating or confirming the data within the record series and for confirming that the particular series was produced in accordance with standard procedures?	

Criteria Group 5: Checklist (5.A)
Metadata Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
5.A.1 Record metadata: unique identifier			
5.A.2 Record metadata: date of creation			
5.A.3 Record metadata: time of creation			
5.A.4 Record metadata: creator/agency/organization			
5.A.5 Record metadata: documentation of creator's authorization			
5.A.6 Record metadata: date of modification			
5.A.7 Record metadata: time of modification			
5.A.8 Record metadata: modifier/agency/organization			
5.A.9 Record metadata: documentation of modifier's authorization			
5.A.10 Record metadata: indication of authoritative version			
5.A.11 Record metadata: identification of originating system			
5.A.12 Record metadata: date of receipt from outside system			
5.A.13 Record metadata: time of receipt from outside system			
5.A.14 Record metadata: addressee			
5.A.15 Record metadata: system or mechanism used to capture record from outside system			

Criteria Group 5: Checklist (5.A)
Metadata Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
5.A.16 Record metadata: protection method			
5.A.17 Record metadata: media type			
5.A.18 Record metadata: format			
5.A.19 Record metadata: location of record			
5.A.20 Record metadata: sensitivity classification			

Data Warehousing Questions	Response
Do you gather extraction metadata?	
Do you cleanse the data?	
Do you document the cleansing procedure?	
Do you gather cleansing metadata?	
Do you transform the data?	
Do you document the transformation procedure?	
Do you gather transformation metadata?	
What metadata/documentation do you offer users?	
Who can access metadata?	
Who can alter metadata?	
Who can delete metadata?	
Who can add metadata?	
What are the legal liabilities regarding data ownership and custodial responsibilities?	
Where do data custody responsibilities reside — with the source systems, the warehouse system, or both?	
Are there records retention schedules and policies for warehouse data?	
Is retention of warehouse data coordinated with retention of data in the source systems?	